NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A
Effective Date: May 16, 2006
Expiration Date: May 16, 2011

Printable Format (PDF)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

Chapter 2 Roles and Responsibilities

2.1 Roles and Responsibilities Overview

2.1.1 To implement the various Federal and NASA policies and requirements, FISMA allows for the delegation of IT Security Program responsibilities to various functional roles. NASA senior managers establish the Agency's IT Security Program and its overall program goals, objectives, and priorities. The NASA IT Security Program involves all staff in some capacity. NASA Headquarters, Centers, and support service contractor sites have the latitude to use their internal organizational structure to fulfill the roles and responsibilities described in this chapter if the approach is documented in policy or guidance. The following roles and responsibilities identify key personnel in the IT Security Program.

2.1.2 NIST provides detailed information on IT security-related roles and responsibilities. These are found throughout each NIST document addressing specific IT security elements.

2.2 Senior Management

2.2.1 Senior IT Security Management

2.2.1.1 Ultimately, responsibility for the success of the NASA IT Security Program lies with its senior managers. They establish NASA's IT Security Program and its overall

goals, objectives, and priorities to support NASA's mission. NASA managers may delegate to others the responsibility of ensuring that IT security controls, requirements, and procedures are implemented, measured, and improved via life cycle processes.

2.2.1.2 High-level roles and major responsibilities are addressed in this section. They establish the basis for the employee's awareness and compliance by following all applicable security practices and expecting the same of others. See Figure 2-1.

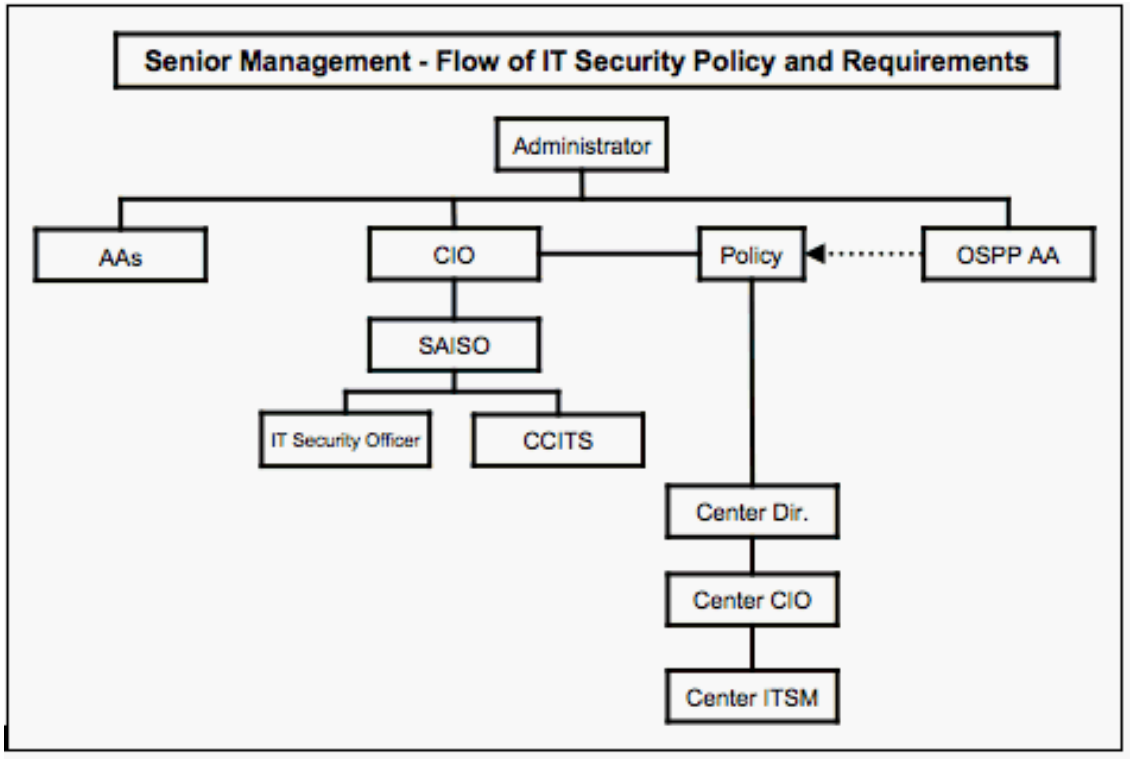

Figure 2-1 NASA Senior IT Security Management Working Relationship

2.2.2 NASA Administrator

2.2.2.1 In accordance with FISMA, the NASA Administrator is responsible for:

a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use disclosure, disruption, modification, or destruction of 1) information collected or maintained by or on behalf of NASA, and 2) information systems used or operated by NASA or by a contractor of NASA.

b. Agency compliance with Section 11331 or Title 40 U.S.C., including related policies, procedures, standards, and guidelines.

c. Agency compliance with information security standards and guidelines for national security systems issued in accordance with law and as directed by the President.

d. Ensuring that information security management processes are integrated with strategic and operational planning processes.

e. Ensuring that senior Agency officials provide information security for the information and information systems that support the operations and assets under their control.

2.2.2.2 To ensure compliance with the responsibilities of 2.2.2.1, the following delegations are effected by the Administrator:

a. The NASA CIO is delegated the authority to coordinate with the NASA Mission Directorate Associate Administrators, Heads of Mission Support Offices, Center Directors, and NASA program managers to reallocate funds as required to ensure compliance with IT security requirements.

b. The Head of the Office of Security and Program Protection (OSPP) is delegated the responsibility for protecting classified national security information.

c. The Agency Principal Accreditation Authority (PAA), as appointed by the NASA Administrator, is delegated responsibility for establishing and implementing a standardized approach for the certification and accreditation of NASA's National Security Systems (NSS), which includes collateral, sensitive compartmented information (SCI), and special access programs (SAP). The PAA shall ensure the implementation of National Security Telecommunications and Information System Security Instruction (STISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP) and duly appoint a Designated Approval Authority (DAA) process for collateral national security systems, as well as appropriate certification and accreditation processes for SCI and SAP national security systems.

2.2.3 NASA CIO

2.2.3.1 The NASA CIO shall maintain an effective and economical information resource management (IRM) program and ensure that standards and policies for using IT resources incorporate effective protection measures. A key element of the IRM program is protecting information resources. To this end, the NASA CIO is responsible for IT security and has the management oversight responsibilities for ensuring the confidentiality, integrity, and availability of IT resources.

2.2.3.2 The NASA CIO shall establish policies and requirements necessary to comply with FISMA and ensure that NASA information and information systems are protected.

2.2.3.3 To accommodate new threats and vulnerabilities, the NASA CIO shall issue NITR documents to keep current with changes in the IT environment and with changes in Federal guidelines.

2.2.3.4 The NASA CIO shall issue directives, as necessary, to measure the effectiveness of IT security activities, collected data, and analyzed information for trends and to report to NASA management and OMB on the status of the NASA IT Security Program.

2.2.3.5 The NASA CIO shall work with the Mission Directorates, Support Offices, Centers, and program managers to reallocate funds to ensure that NASA complies with FISMA and OMB directives.

2.2.3.6 To implement the NASA-wide IT Security Program effectively, the NASA CIO shall:

a. Appoint a Deputy CIO for IT Security to fill the FISMA role of Senior Agency Information Security Officer (SAISO) and to establish and implement the NASA-wide IT Security Program.

b. Delegate to the OSPP the responsibility for establishing and managing the certification of IT Systems advocate.

c. Establish the NASA Enterprise Architecture to integrate IT security into the strategic planning, capital planning and investment processes.

d. Establish a Competency Center for IT Security (CCITS) to advise and support the SAISO, NASA Authorizing Officials (AOs), Mission Directorate CIOs, Center CIOs, and Center IT Security Managers (ITSMs).

e. Establish a CIO Board to review Agencywide systems to ensure a consistent implementation of security requirements.

f. Provide IT security advice and support to the CPIC processes.

2.2.4 NASA Deputy CIO for IT Security/Senior Agency Information Security Officer

2.2.4.1 The Deputy CIO for IT Security serves as the SAISO. The SAISO is responsible for implementing the IT Security Program of NASA and providing advice and assistance to the Administrator, the NASA CIO, and other senior Agency personnel with IT security roles and responsibilities. The SAISO interacts with external groups regarding IT security, including OMB, Congress, and other Federal agencies and entities exhibiting IT security best practices and plays a leading role in introducing an appropriate, structured methodology to help identify, evaluate, and minimize information security risks.

2.2.4.2 The SAISO shall manage, coordinate, and maintain the overall direction and structure of the NASA IT Security Program.

2.2.4.3 The SAISO shall establish SOPs to provide implementation guidance to ensure consistency of IT security objectives and solutions.

2.2.4.4 The SAISO shall recommend NITRs as interim policy and requirements necessary to address new issues and to clarify existing policy and requirements.

2.2.4.5 The SAISO shall:

a. Appoint an IT Security Officer to oversee and direct NASA-wide IT Security Services such as the IT Security Awareness and Training Center, the NASA Incident Response Center (NASIRC), and the NASA Security Operation Center (NSOC).

b. Oversee, direct, and approve the activities of the CCITS by establishing a Cost, Schedule, and Performance Agreement (CSPA).

c. Charter, oversee, and chair a Network Security Control Board (NSCB) to focus on changes that affect the IT security of NASA at the demarcation of the Agency's Wide Area Network (WAN) and external connectivity. The NSCB will also address IT security network changes within that affect multiple centers. The SAISO shall approve the membership on the NSCB. The SAISO can delegate the role of NSCB Chair.

d. Establish expert centers and ad hoc working groups, as necessary, to assist in developing and implementing the NASA IT Security Program.

e. Provide advice and assistance to the Administrator, NASA CIO, program managers, and other senior Agency personnel to ensure that Agency IT security goals, priorities, and requirements are effectively addressed to protect NASA's investment in IT resources.

f. Recommend metrics to the NASA CIO to measure the IT security posture of NASA to comply with Federal requirements.

2.2.4.6 The SAISO shall review the CPIC processes to ensure that:

a. NASA's Exhibit 300s and Exhibit 53s submitted to OMB identify and adequately

provide for implementing IT security requirements.

b. Master and subordinate IT systems map to investments as defined by OMB Exhibit 53 or Exhibit 300.

2.2.4.7 The SAISO shall coordinate with the OSPP to ensure that the IT security assessment and certification activities are adequately supporting the NASA CIO in complying with FISMA and OMB requirements.

2.2.4.8 The SAISO shall track progress of all master and subordinate IT system POA&M items whose scheduled completion date may impact NASA's compliance with FISMA and OMB requirements and report to the NASA CIO in time for corrective action to be taken.

2.2.4.9 The SAISO shall provide a mechanism to ensure that all IT resources comply with standard operating system benchmark templates. NASA will evaluate each system's operating system through a vendor-provided benchmarking capability.

2.2.4.10 The SAISO shall work closely with the Office of Procurement in the development of Agencywide IT security clauses and provisions for incorporation into requests for proposals, requests for quote and statement of work, and other solicitations and procurement and non-procurement instruments.

2.2.5 Office of Security and Program Protection

2.2.5.1 The OSPP is responsible for all aspects of classified national security information matters, including establishing the certification and accreditation policies, procedures, and guidance for all classified IT systems operations. The OSPP responsibilities also include providing the OCIO with support in assessing and certifying unclassified IT systems and ensuring compliance with FISMA and Federal requirements.

2.2.5.2 The Assistant Administrator for OSPP shall:

a. Establish personnel screening policies and requirements for access to IT resources.

b. Ensure that the NASA Counter Intelligence (CI) Program coordinates with the Center ITSMs on matters regarding threats to NASA IT systems and network infrastructure.

c. Coordinate with the SAISO, the CCITS Manager, and NASIRC in the issuance of IT security alerts regarding potential threats and exploits that could affect NASA IT resources and network infrastructure.

d. Support the C&A process and assessments of unclassified IT systems with personnel security and physical security experts and advice.

e. Cooperate with the NASA Office of Inspector General (OIG) on law enforcement matters dealing with cyber counterintelligence (CI) and cyber espionage investigations in accordance with NPR 1600.1, NASA Security Program Procedural Requirements.

f. Appoint an Information Assurance Officer (IAO) to implement an information assurance program to:

(1) Provide internal assessments of IT security policy compliance.

(2) Establish a certification program for systems with an IT security category of moderate or high, in compliance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

(3) Issue requirements for the protection, handling, and destruction of administratively controlled information (ACI) or sensitive but unclassified (SBU) information.

2.2.5.3 The Deputy Assistant Administrator for OSPP is assigned the role of AO for OSPP's master systems and shall:

a. Make the security accreditation decisions for OSPP master systems, which establish the IT security posture of the master and their subordinate systems.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA Chief Financial Officer (CFO) and CIO that funding be redirected to implement security controls required for master or subordinate systems to achieve full Authorization to Process (ATO).

d. Concur or non-concur on the determination of master system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls which will be inherited by any subordinate system under the authority of the master system.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.2.6 NASA IT Security Officer (ITSO)

2.2.6.1 The ITSO shall ensure the effectiveness of:

a. NASA IT security projects crossing Centers.

b. The collecting, analyzing, and reporting of metrics established by the OCIO.

c. The NASA IT Security Awareness and Training Program.

d. NASIRC.

e. The NASA WAN services.

2.2.6.2 The ITSO shall oversee, direct, and approve the activities of the SAISO established NASA IT Security Projects via establishing CSPAs.

2.2.6.3 The ITSO shall recommend metrics to the SAISO to measure the IT security posture of NASA to comply with Federal requirements.

2.2.7 Manager, Competency Center for IT Security

2.2.7.1 The Competency Center for IT Security (CCITS) is the NASA CIO's authorized organization to perform Agencywide IT security leadership, develop and oversee IT security initiatives program management, and perform technology investigation to ensure NASA's pre-eminence in securing its information technology resources with minimal risk and highest efficiency.

2.2.7.2 The CCITS Manager shall:

a. Annually develop a CCITS CSPA that is responsive to the NASA and CIO priorities and directions.

b. Report to the NASA SAISO and be accountable for project schedule, budget, and deliverables, and understand and adhere to the above operating structure of the CSPA.

c. Communicate regularly with the NASA SAISO to ensure that the IT security recommendations, goals, schedules, and budgets are current and on track.

d. Report on progress against the CSPA at least quarterly.

e. Involve NASA Mission Directorate, Centers, and other stakeholders to ensure the timely introduction of new or revised standards or new services with the goal of implementing technically superior solutions, cost effectiveness, and minimal disruption or negative impact upon the IT operational infrastructure and programs of NASA.

f. Continually engage constituencies from other NASA Centers and other Agencies in the definition and implementation of architectures, standards, guidelines, and services.

2.2.8 Center Directors and the Assistant Administrator for Infrastructure and Administration

2.2.8.1 Center Directors and the Assistant Administrator for Infrastructure and Administration are responsible for protecting the Center's missions and programs, advocating support for IT security requirements, and providing the resources necessary to implement the IT security requirements.

2.2.8.2 The Center Directors and the Assistant Administrator for Infrastructure and Administration shall:

a. Delegate the responsibility for the Center IT security program to the Center CIO.

b. Provide adequate funding to programs/projects to implement the Center IT security program and to be compliant with FISMA and NASA requirements.

c. Appoint an ITSM to assist the Center CIO by providing organization and direction for implementing the NASA IT security program.

d. Ensure that IT capital planning and investments address and fund IT security requirements.

e. Ensure that employees and support service contractors are held accountable for adhering to IT security policies and requirements.

f. Ensure IT investments comply with the NASA Enterprise Architecture.

g. Ensure the Center Privacy Act Manager works with the Center ITSM and IAO to protect information subject to the Privacy Act.

2.2.9 Center Chief Information Officer

2.2.9.1 The Center CIO is responsible for establishing an effective and economical Center Information Resource Management (IRM) program. The IRM program plan defines the design and operation of the Center's information infrastructure (e.g., networks, servers, and electronic forms) and ensures alignment with the NASA IRM's vision, mission, and strategy. The Center IT security roles and responsibilities shall

reside within the Center CIO office.

2.2.9.2 The Center CIO shall:

a. Establish and chair the Center Network Configuration Control Board (NCCB) to conduct a risk assessment for modifications to the network, to approve or disapprove all modifications, and to provide notification to its customers of all modifications that would affect the protections provided by the network. The Center CIO may delegate the NCCB chair function.

b. Ensure that civil service Organization Computer Security Officials (OCSOs) have the appropriate knowledge, skills, and abilities and are assigned to facilitate the implementation and oversight of the IT security of systems within their organization. For non-NASA facilities or organizations, a non-civil servant may serve as an OCSO.

c. Provide the Center ITSM with sufficient resources to ensure Center compliance with IT security requirements.

d. Manage the Center's network infrastructure to protect information system owners and to control unauthorized internet protocol (IP) addresses.

e. Establish an IT security incident response capability that is accountable to the Center ITSM.

f. Designate a Center-wide certification agent (CA) who shall:

(1) Oversee and assist information system owners in the self-assessments process required for certification.

(2) Assist information system owners in determining information security categories for systems.

(3) Assist information system owners in determining the appropriate system boundaries and security controls.

(4) Ensure that the activities and documentation required in the initiation phase of the C&A process are completed.

g. Delegate to the Center ITSM the authority to determine when an IT security incident is placing NASA's missions, its customers, its reputation, or its assets in immediate jeopardy to a degree that the Center must exercise its responsibility to unilaterally control or terminate incidents. Actions should be coordinated prior to being implemented with the Center CIO, Center Chief of Security (CCS), the OIG, impacted information system owners, and Information System Security Officials (ISSOs), as soon as practicable.

2.2.9.3 The Center CIO is assigned the role of the AO for the following IT systems.

a. Office Automation of Information Technology (OAIT) subordinate systems;

b. OSPP subordinate systems.

c. Multi-Program subordinate systems (i.e., systems supporting multiple Mission Directorates who share the operating cost, but where no Mission Directorate funds a majority portion of the operational cost).

2.2.9.4 The Center CIO, as an AO, shall:

a. Make the security accreditation decisions for the relevant master systems, which establish the IT security posture of the master and their subordinate systems.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA CFO and CIO that funding be redirected to implement security controls required for the subordinate systems to achieve full authorization to operate (ATO).

d. Concur or non-concur on the system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls inherited from the master system. Non-concurrences shall indicate that the system needs to be aligned with a different master or that a new master system must be created.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.2.10 Center IT Security Manager

2.2.10.1 The Center ITSM is responsible for implementing the Center IT Security Program. The Center ITSM's role is to develop Center-wide IT security policies and guidance, to coordinate and facilitate IT security awareness and training, to maintain an incident response capability, and to document, review, and report the status of the Center IT Security Program.

2.2.10.2 The Center ITSM shall:

a. Support the Center CIO to ensure compliance with NASA policies, requirements, and directives from the OCIO.

b. Develop Center-wide IT security policies and guidance for approval by the Center CIO.

c. Assist Center organizations on all aspects of IT security throughout the life cycle of their IT systems.

d. Conduct periodic assessments and compliance checks.

e. Maintain and track the status of all system security plans (SSPs) assigned to their Center for compliance with NIST and guidance from the NASA SAISO.

f. Track and report the Center's POA&M and IT security metrics status to Center and Agency management.

g. Implement Center vulnerability scanning, patch management, operating system configuration, and penetration testing program to ensure that controls are in place and effective.

h. Develop an incident response capability in coordination with the CCS and the OIG, following the guidance provided by the SAISO for handling and reporting incidents.

i. Coordinate and facilitate the Center IT security awareness and training program.

j. Be an advisor to the chair of the Center NCCB and a member of the Center's NCCB.

k. Have the authority to disconnect or deny service to any network attached device, including wireless, in the event of an incident or violation of acceptable use policy.

l. Provide the Procurement Office with IT security requirements to support preparation of solicitation documents.

2.3 IT Security System and Information Owners

2.3.1 Many individuals at both the Agency and Center levels have key roles to oversee the implementation of a sound IT Security Program within their areas of responsibility. See Figure 2-2.

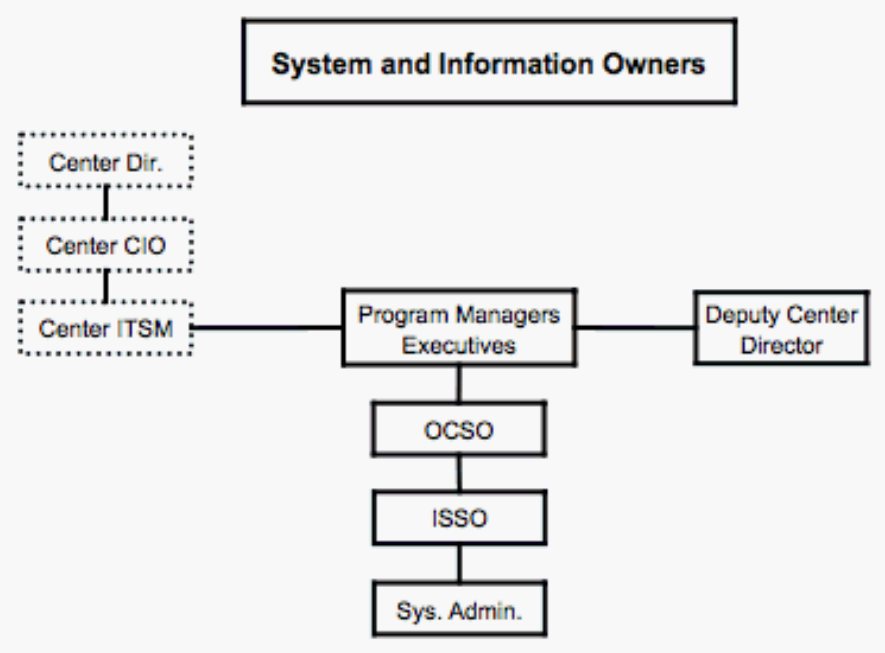

Figure 2-2 IT Security System and Information Owners

2.3.2 Project/Program/Functional Managers as Information System Owners

2.3.2.1 Every IT system has an information system owner who is responsible for the successful operation and protection of the system and its information. Program, project, and functional managers are often identified as the information system owners. Information system owners are usually civil service personnel; but can be support service contractors or partners under agreements with NASA. In addition, there can be information owners who entrust their information and applications to information system owners to process, store, and handle. Information system owners and information owners are responsible for ensuring that the system development life cycle (SDLC) security requirements are identified during the system's initiation phase, addressed throughout design reviews, tested and verified during implementation and operational phases, and maintained during the disposition phase.

2.3.2.2 A civil service manager shall oversee the IT security of the systems or applications that are operated and managed through a support service contract, contractor, grant, or agreement. For government-owned contractor-operated (GOCO)

facilities (e.g., Jet Propulsion Laboratory), a non-civil service individual, at an equivalent civil service management level, may serve as the on-duty line manager.

2.3.2.3 Information System Owners (i.e., Program and Project Managers or their designee) shall:

a. Ensure that their system complies with the mandatory requirements of NPR 7120.5, NASA Program and Project Management Processes and Requirements, and with the IT security requirements controls to ensure protective safeguards are addressed early and throughout the system's life cycle.

b. Report systems costing more than $500,000 on the Center's "Capital Asset Plan and Business Case," Exhibit 300.

c. Ensure that the project and program plan, where applicable, integrates security throughout the life cycle, including the processes and procedures of NPR 7120.5, NASA Program and Project Management Process and Requirements.

d. Ensure their systems are designed and implemented in accordance with the NASA Enterprise Architecture.

e. Work with all their Information Owners, following the NIST guidance in developing the contingency requirements for their systems.

f. Ensure their systems comply with the C&A requirements identified in Chapter 14, System Certification and Accreditation, and provide adequate resources to meet these C&A requirements.

g. Ensure that all interconnected systems (i.e., systems owned by another organization) have an Interconnection Memorandum of Understanding (MOU) and Interconnection Security Agreement in place, which define the rules of behavior and controls that must be maintained for system interconnection and that these are included in the IT SSP.

h. Oversee the overall compliance of their assets with their defined/identified security requirements by ensuring that proper ITS controls are in place.

2.3.3 Information Owners

2.3.3.1 All NASA information has an owning organization responsible for its confidentiality, integrity, and availability. Although Information Owners may have their information processed by another organization, support service contractor, or partner, the NASA Information Owners shall be ultimately accountable and responsible for understanding any risk that another manager has accepted for the system processing their information.

2.3.3.2 Information owners shall:

a. Understand the IT security strategy, contingency requirements, and security risks of systems that process, store, and handle their information.

b. Be responsible for a program or function (e.g., procurement or payroll) including the supporting IT resources and provision of appropriate management, operational, and technical controls. This includes the information supporting a program or function regardless of whether the information is processed by another organization or contractor.

c. Play an essential role in IT security relative to strategic planning initiatives and be intimately aware of functional service requirements of the system supporting their information.

d. Ensure programmatic IT security interests are addressed during the IT security services life cycle.

e. Oversee the overall compliance of their assets with their defined/identified security requirements.

f. Concur or non-concur on the C&A decisions.

g. Retain the accountability and responsibility by ensuring rules of behavior are propagated that protects their information even when the information is shared with other organizations.

h. Ensure that all interconnected systems are documented and have signed agreements in place in accordance with NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, and Chapter 9, System Interconnectivity.

2.3.4 Organization Computer Security Official

2.3.4.1 An Organization Computer Security Official (OCSO) is responsible for a particular organization's IT Security Program. The OCSO serves as the critical communication link to and from that organization and its programs for all IT security matters.

2.3.4.2 The OCSO shall:

a. Serve as the organization's representative to the Center ITSM, representing the organization's director or office chief on all IT security matters and advising the Center NCCB on the possible impact from modifications in the IT network infrastructure.

b. Periodically report the status of the organization's IT security posture and concerns to the Center ITSM and the organization's senior manager.

c. Ensure the organization complies with NASA and Center IT security requirements, and notify the Center ITSM if there is an obstacle to meeting requirements, deadlines, or metrics.

d. Review annually the IT SSPs for the organization's systems identifying any changes that would require an update, such as changes in personnel, software and hardware, function, categories of information, information ownership, or risk, and verify the viability and the date of the last test of the contingency plan.

e. Report suspected and actual IT security incidents to the Center ITSM and line management, in accordance with Center-established incident response procedures.

f. Ensure compliance with OSPP requirements for media sanitization by the establishment of a process to ensure that storage media is purged of any data or information that has not been approved for public release prior to releasing the media outside the Center's control.

2.3.5 Information System Security Official

2.3.5.1 The information system security official (ISSO) is the principal staff advisor to the information system owner on all matters involving the IT security of the information

system. This responsibility may also include physical security, personnel security, incident handling, and security training and education. For smaller systems, a system administrator may perform the ISSO role as well as the system administrator role.

2.3.5.2 The ISSO shall:

a. Ensure the security of an information system throughout its life cycle.

b. Play an active role in developing and updating the security plan for the information system as well as in managing and controlling changes to the system and assessing the security impact of those changes.

c. Cooperate in the development and implementation of security tools and mechanisms and other techniques consistent with NASA and Center standards to mitigate vulnerabilities for which there is no countermeasure.

d. Perform annual self-inspections of their systems and report the findings to their line managers, information system owner, and the cognizant OCSO.

e. Conduct system vulnerability checks to ensure that known vulnerabilities and exploits are identified and corrected and that residual risks are documented.

f. Periodically use tools to verify and/or monitor compliance with the NASA password policy for systems under their authority.

g. Ensure effective and timely incident reporting of all incidents and suspected incidents in accordance with Center procedures.

2.3.5.3 ISSO shall ensure appropriateness of user accounts by:

a. Ensuring that all users, administrators, and operators complete an account request document, which is approved by a NASA management official responsible for the individual (e.g., manager, sponsor, task manager) and by the line manager responsible for the system.

b. Promptly disabling access to a user's account if the user is identified as having left the Center, changed assignments, changed contracts, completed work on a grant or other agreement, or no longer requires system access.

c. Granting accounts only to individuals who have had the appropriate personnel screening in accordance with NPR 1600.1, NASA Security Program Procedural Requirements.

d. Ensuring that foreign nationals have approval by the CCS in coordination with the Center CIO, the Export Control Officer, and the information system owner prior to being granting access. Approval is required for access to every system.

e. Granting privileged, limited privileged, or non-privileged access to each system by foreign nationals or foreign representatives only with the written concurrence of the Center's Chief of Security and the information system owner.

2.3.6 System Administrator

2.3.6.1 NASA civil service and support service contract system administrators are the managers and technicians who design and operate information technology resources for their respective NASA Centers. They are often a part of a larger Information Resources Management (IRM) organization. They usually have privileged access to NASA

information resources.

2.3.6.2 Each system administrator shall:

a. Ensure that security controls, as described in the SSP, are properly implemented throughout the system's life cycle.

b. Maintain configuration profiles of all systems controlled by the organization including, but not limited to, mainframes, distributed systems, microcomputers, and dial-up and wireless access ports.

c. Implement all system changes required to protect their systems, including system patches as soon as they are available and tested to remove vulnerabilities. Systems, which are under a launch or mission freeze, must address this requirement immediately following the lifting of the freeze.

d. Monitor system integrity, protection levels, and security-related events; resolve detected security anomalies associated with their information system resources; conduct security tests as required; and assess and verify the implemented security controls.

e. Follow the Center's incident response procedures.

f. Be certified by the NASA System Administrator Certification Program in the particular operating system(s) for which they are responsible and in network and internet security practices.

g. Place the NASA CIO-approved warning banner on all systems that are owned by or operated on behalf of NASA.

2.4 Center IT Security Supporting Functions

IT security supporting functions are those functional roles that have a responsibility in ensuring that IT security policies, procedures, and requirements are implemented in their area of accountability. See Figure 2-3.

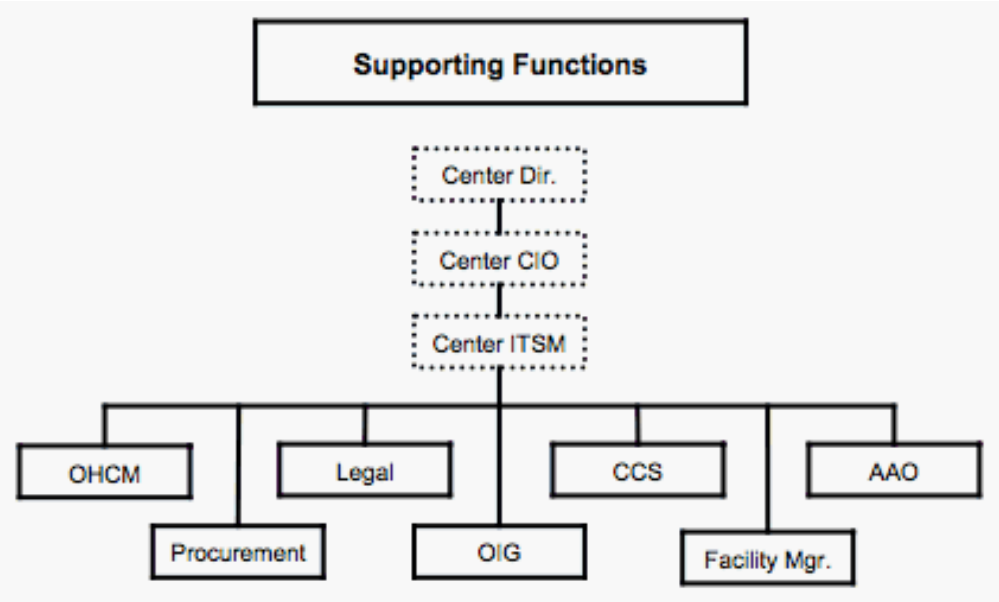

Figure 2-3 Center IT Security Supporting Functions

2.4.1 Head, Office of Human Capital Management

2.4.1.1 A partnership exists between the Office of Human Capital Management (OHCM) and the NASA CIO to further IT security curriculum development and the delivery of training for civil servants, including required training for support service contractors.

2.4.1.2 The Head of OHCM shall:

a. Ensure that all new civil service employees receive IT security awareness training prior to being released to their supervisor.

b. Ensure that all civil service employees assigned to management positions complete IT security awareness training for managers prior to assuming duties as a manager.

c. Advise management on administrative actions available for non-compliance with mandatory IT security requirements.

d. Work closely with managers and the CCS on issues involving the determination of position sensitivity and degrees of background investigations required for a particular position.

e. Provide security-related exit procedures when employees leave a NASA organization.

2.4.1.3 Head, Center's Training Office shall:

a. Provide reports quarterly to the Center CIO, Center ITSM, and the IT Security Awareness and Training Center on the status of employee training metrics.

b. Maintain records of civil service personnel who have taken training.

c. Maintain a schedule of when follow-on training will be required.

d. Track the status of employee training metrics.

e. Budget funds and resources for both initial and follow-on Center-specific IT security curricula.

2.4.2 Procurement Officers

2.4.2.1 The Procurement Officers are responsible for ensuring that solicitations and procurement and non-procurement instruments incorporate Federal and NASA clauses and provisions. Joint processes, developed in coordination with the SAISO and the ITSO, shall be established for verifying that IT security is specifically addressed in the initiation of solicitations and procurement and non-procurement instruments.

2.4.2.2 Procurement Officers shall:

a. Verify that NASA IT security requirements, as identified in the NASA FAR Supplement, are included in solicitations and procurement and non-procurement instruments or specifically documented as not being appropriate by the funding organization.

b. Direct those initiating contracts and other solicitations and procurement and non-procurement instruments to their CIO and ITSM for assistance in documenting the information security category and understanding the resulting impact level, required security controls, and budget considerations.

2.4.3 Contracting Officers Technical Representative (COTR)

2.4.3.1 The COTR shall:

a. Obtain the advance coordination of the cognizant ITSM of the issuance of contract modifications or new task orders, which will involve operation, use, or access to Federal or NASA IT resources or information.

b. Establish a process for notifying the Center Account Authorization Official (AAO) and the Center ITSM when any contractor employee is terminated or otherwise no longer requires system access.

c. Establish processes to verify that all contractor employees complete the require IT security awareness training, as specified in the contract, prior to being granted access to NASA IT systems, information, or data.

d. Work closely with system owner and the CCS when determining the position sensitivity and the required degrees of background investigations required for all contractor positions. (See Chapter 4, Section 4.5 of NPR 1600.1, NASA Security Program Procedural Requirements, for more information.)

2.4.4 General Counsel

2.4.4.1 The General Counsel shall:

a. Advise the CIO regarding IT security policies and provide procedures for legal compliance.

b. Provide managers with legal advice regarding non-compliance with IT security policy.

c. Be responsible for advising the acquisition team on legal issues associated with the procurement.

2.4.4.2 The General Counsel shall review and approve non-disclosure agreements to ensure they are consistent and to ensure they provide adequate protection for NASA ACI/SBU information.

2.4.5 Center Chief of Security

2.4.5.1 The Center Chief of Security (CCS) shall:

a. Conduct appropriate personnel security screening for those working in high impact or critically sensitive positions, which includes those who can bypass IT technical security controls and processes.

b. Coordinate, investigate, and approve requests for foreign nationals and international partners who require privileged or non-privileged access to systems, applications, and networks operated by or on behalf of NASA.

c. Develop a process that alerts the appropriate account management officials and the organization ISSO or OCSO of persons having access to IT information and resources leaving employment and exiting the Center.

d. Ensure the physical security of Center IT resource facilities.

2.4.5.2 The CCS, in coordination with the OSPP CI Officer, shall establish a process to gather intelligence information regarding threats toward IT resources and provide this information to the Center ITSM and the CIO. The Center CIO shall ensure that the information system owner is informed.

2.4.5.3 The CCS shall approve access to IT resources, in accordance with NPR 1600.1, NASA Security Program Procedural Requirements, for all foreign nationals.

2.4.6 Office of Inspector General

2.4.6.1 The Office of Inspector General's (OIG's) role in IT security is to investigate computer crimes for possible prosecution in court and to conduct audits of IT resources for proper management, which includes appropriate protective controls. In this role, the OIG shall:

a. Promptly notify appropriate NASA management of incidents whenever the OIG has reason to believe, or is aware, that there is a threat to human safety or critical missions.

b. Coordinate, to the greatest extent practicable, with the Center CIO and ITSM, when use of Center computer or network data is needed to support an investigation that is being conducted.

c. Investigate, as appropriate, incidents forwarded by the Center ITSM, which constitute a computer crime.

d. Serve as the focal point for referrals to the Department of Justice and other external law enforcement organizations of all violations of Federal criminal and civil statutes related to computer system intrusions or criminal misuse of computers.

2.4.7 Building or Facility Manager

2.4.7.1 Building or facility managers are responsible for ensuring the provision of such services as electrical power and environmental controls necessary for safe and secure system operations. Often, separate medical, fire, hazardous waste, or life safety personnel augment these managers.

2.4.7.2 Building or facility managers shall:

a. Ensure that physical access controls protecting information systems are correctly installed, maintained, and tested annually.

b. Ensure that safety controls are managed and tested annually.

c. Ensure that HVAC controls are adequate for IT system availability requirements, are maintained, and are tested.

d. Support the certification of IT security controls. Security controls are the management, operational, and technical controls prescribed for information contained in an information system which, when taken together, satisfy the specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and the information.

2.4.8 Center Account Authorization Official

2.4.8.1 The Center Account Authorization Official (AAO) serves as the primary technical representative for account management issues and provides guidance and oversight of the daily activities of all Center staff supporting the NASA Account Management System (NAMS).

2.4.8.2 Center AAOs shall:

a. Have the authority and responsibility for all aspects of policy, business operations, and operational life cycle for NAMS.

b. Provide guidance and oversight of the account management activities.

c. Enforce NIST SP 800-53, Recommended Security Controls for Federal Information Systems, and NASA security controls and requirements for NAMS passwords.

d. Work with the Center ITSM on security issues, compliance, and support.

e. Report known or suspected security incidents to the Center ITSM, in accordance with Center procedures.

2.4.9 User Community and NASA Customers

2.4.9.1 Because NASA resources, information, data, and processing systems are held in public trust, the NASA user community and NASA customers share responsibility for protecting these IT resources. Policies and requirements cannot always be implemented through automated technical controls. Consequently, individuals shall voluntarily comply with procedures by agreeing to accept NASA's Appropriate Use Policy Statement (See Section 11.3.3, Appropriate Use of IT Resources).

2.4.9.2 Users of NASA systems or information shall:

a. Comply with the requirements for limited personal use and inappropriate use described in Section 11.3.4, Limited Personal Use of IT Resources. If users are unsure about whether an activity is permitted, they should consult with their Center ITSM.

b. Comply with existing laws and policies that restrict the distribution of ACI and SBU information. (See the procedures described in NPR 1600.1, NASA Security Program Procedural Requirements.)

c. Be responsible for ensuring their sponsored guests and visitors are aware of Center policies, procedures, and requirements regarding the use of NASA IT resources, including wireless access.

d. Comply with NASA password policies as described in Section 11.3.7, Password Requirements, and NASA incident handling policies and procedures as described in Chapter 17, Security Incident Handling and Reporting.

e. Users of NASA information systems or those having access to NASA information shall immediately report any known or suspected IT security incidents, following the Center's procedures for incident reporting. It is the responsibility of the OCSO or information system owner to notify the Center ITSM of all known or suspected incidents.

f. Complete mandatory basic IT security awareness training prior to accessing NASA systems and applications and annually thereafter as long as access to NASA information or IT resources continues.

2.5 Certification and Accreditation Roles

2.5.1 The role of the Agency Authorizing Official in the accreditation process is detailed in Section 14.5, Accreditation Process Requirements.

2.5.2 Authorizing Official (AO) Requirements

2.5.2.1 The AO is the NASA management official with the authority to approve the operation of the information system at an acceptable level of risk to NASA operations (including mission, functions, image, or reputation), agency assets, or individuals.

2.5.2.2 The AO, by relying on themselves or IT security professionals, shall:

a. Be knowledgeable in computer, telecommunications, and networking technology, as well as security methods and practices. NASA will provide role-based AO training.

b. Have the authority to:

(1) Oversee the budget and business operations of the information system within the NASA organization and have the authority to allocate resources to achieve an acceptable level of security, to remedy security deficiencies, or to halt processing.

(2) Approve security requirements documents, security plans, memorandums of agreement (MOA), memorandums of understanding (MOU), and any authorized or allowable deviations from security policies.

(3) Allocate resources to achieve an acceptable level of security.

(4) Remedy security deficiencies.

(5) Halt processing when conditions warrant.

c. Assume responsibility and accountability for the risks of operating the information system in a specific environment through the completion of the accreditation process and be accountable for both the system and for adverse impacts to NASA if a breach of security occurs.

d. Ensure the C&A process is performed during life cycle changes of systems, when a significant change is determined to affect security, and at least every three years prior to the expiration of the last C&A.

e. Establish the minimum baseline security controls for their IT security systems.

f. Ensure that the C&A process is followed prior to granting a full Authorization to Operate (ATO) or an Interim Authorization to Operate (IATO). This includes when a significant change is determined to affect security and at least every three years prior to the expiration of the last C&A.

g. Grant one of three types of accreditation decisions, which are more fully explained in Section 14.4, Accreditation Process, upon completion of the C&A process:

(1) Authorization to operate the system once the certification process has been completed.

(2) Issue an IATO to operate the system under specific terms and conditions.

(3) Deny authorization to operate the system (or if the system is already operational, halt operations) if unacceptable security risks exist.

h. Require information system owners whose systems have interim accreditations or operational denial to provide documentation on the corrective actions to be taken and the timeline for completion in order to achieve full accreditation or to resume operations.

i. Establish agreements among the AOs, if multiple AOs are involved, and document in

the security plan.

2.5.2.3 Authorizing Officials for master system plans shall:

a. Make the security accreditation decisions for their master systems which establish the IT security posture of the master and their subordinate systems.

b. Explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

c. If necessary, advocate to the NASA CFO, NASA CIO, and applicable program office that funding be redirected to implement security controls required for master or subordinate systems to achieve full ATO.

d. Concur or non-concur on the determination of a master system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls which will be inherited by any subordinate system under the authority of the master system.

e. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

f. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.5.2.4 Authorizing Officials for subordinate systems plans shall:

a. Make the security accreditation decisions for the subordinate systems, which establish the IT security posture of the subordinate system and explicitly accept the risk to NASA operations, assets, or individuals based on the implementation of an agreed-upon set of security controls and IT security strategy of the system.

b. If necessary, advocate to the NASA CFO, NASA CIO, and applicable program office that funding be redirected to implement security controls required for the subordinate systems to achieve full ATO.

c. Concur or non-concur on the system's boundaries, the IT security category, the information type, initial risk assessment, and the selection of security controls inherited from the master system. Non-concurrences shall indicate that the system needs to be aligned with a different master system or that a new master system must be created.

d. Make the security accreditation decision and sign the accreditation decision letter accepting risk for NASA.

e. Not delegate the role of AO, but, if required, may delegate other supporting accreditation activities, such as reviewing and verifying documents.

2.5.3 Certification Agent Requirements

2.5.3.1 The independence of the Certification Agent (CA) is an important factor in assessing the credibility of the security test and evaluation results and ensuring that the AO receives the most objective information possible in order to make an informed, risk-based security accreditation decision.

2.5.3.2 The CA shall be appointed to preserve the impartial and unbiased nature of the security certification as follows:

a. For high and moderate impact systems, the Agency independent third-party shall be identified by the SAISO with concurrence by the OSPP.

b. For a low impact level system, the CA can be selected from the system support staff.

2.5.3.3 The Certification Agent shall:

a. Provide an independent assessment of the security plan to ensure the plan provides a complete and consistent security specification for the information system, prior to initiating the security test and evaluation activities.

b. Conduct a comprehensive assessment of the management, operational, and technical security controls of the information system to determine the effectiveness of those controls in a particular environment of operation and the vulnerabilities in the system after the implementation of such controls. A comprehensive assessment means the review and analysis of all the security controls identified as "baseline security controls for the impact level" as identified in SP 800-53 shall be reviewed and analyzed.

c. Review the results of testing of selected security controls, summarize results, and identify residual risks and impacts.

d. Provide recommended corrective actions to reduce or eliminate vulnerabilities in the information system.

e. Prepare an Accreditation Package consisting of a Certification Letter of Recommendation, a Risk Assessment Summary, and an IT SSP for the AO.

f. Be supported by a certification team providing the essential assessment capabilities necessary to complete the evaluation of the security controls, depending on the size and complexity of the information system and NASA's requirements.

| TOC | Preface | Chapter1 | Chapter2 | Chapter3 | Chapter4 | Chapter5 | Chapter6 | Chapter7 | Chapter8 | Chapter9 | Chapter10 | Chapter11 | Chapter12 | Chapter13 | Chapter14 | Chapter15 | Chapter16 | Chapter17 | Chapter18 | Chapter19 | Chapter20 | Chapter21 | AppendixA | AppendixB | ALL |

| NODIS Library | Legal Policies(2000s) | Search |

DISTRIBUTION:
NODIS